

AI Policy

What is the purpose of this policy?

The On Q Recruitment AI policy establishes principles for the ethical, responsible and effective use of AI systems. It ensures alignment with our mission and values.

Specifically, this policy aims to:

- protect the rights of stakeholders
- support the use of AI to enhance service delivery and achieve our strategic objectives
- ensure transparency in our AI practices so we can maintain public confidence
- provide a clear risk framework for identifying, assessing and managing the risks associated with AI systems
- provide new opportunities to engage and empower our staff.

Scope

This policy applies to:

- all On Q Recruitment permanent and on-hired temporary workers/ contractors and any individuals acting on behalf of On Q Recruitment.
- all AI technologies under On Q Recruitment's control, including those developed inhouse, purchased from vendors or embedded within larger software platforms including cloud based systems.

We define an **AI system** as any technology that uses data to make inferences and generate outputs such as predictions, recommendations, or decisions with a degree of autonomy.

This includes, but is not limited to:

- machine learning models
- generative AI tools
- predictive analytic systems
- chatbots that generate their own responses.

It excludes:

- standard spreadsheet formulas
- rule-based automations (such as 'if-then' macros)
- traditional business intelligence dashboards.

If you are uncertain about whether an AI technology falls under this policy, consult the AI policy owner.

Policy statements

The following AI governance statements set On Q Recruitment's expectations for the responsible design, adoption and use of AI systems across the organisation. They should guide decision-making, promote ethical practices, and ensure AI use aligns with our mission, values, and stakeholder obligations.

These statements apply to all AI systems within scope and must be interpreted in conjunction with our broader risk management, privacy, and technology governance frameworks.

1. Ethical and human-centered use

AI systems must align with our values, respect human dignity and empower human judgment for ultimate decision making.

All uses of AI systems must reflect [Australia's AI Ethics Principles](#) and our values and contribute positively to our mission. AI must not be used to deceive or manipulate stakeholders.

2. Clear accountability

Each AI system must have a designated Accountable Person who has sufficient understanding of the system, its intended use, associated risks, and applicable compliance obligations. The Accountable Person is responsible for overseeing the system's use, ensuring compliance with this policy, and managing any identified risks or issues arising from the system's operation.

An Accountable Person must be appointed before any AI system is adopted or implemented. Unless otherwise approved by the Leadership Team, the Business Operations Manager will be the default Accountable Person for AI systems used within On Q Recruitment. Responsibility may be delegated to another appropriately qualified employee where they are better placed to oversee a specific AI system.

The appointed Accountable Person, together with the scope of their responsibilities, must be recorded in On Q Recruitment's AI Register. This record must be supported by documented risk assessments and any required approvals.

Where an AI system involves third parties, including vendors, developers, or service providers, responsibilities and accountabilities must be clearly documented and allocated between all relevant parties. These arrangements must be reflected in contractual documentation, service agreements, or other appropriate records and maintained within the AI Register.

3. Risk and impact assessment

An AI system must go through a risk and impact assessment before we begin to use it. There must be controls in place that are appropriate the level of risk we are taking on.

Relevant stakeholders should be engaged to understand potential impacts, particularly on vulnerable or marginalised groups.

4. Quality, reliability and security

An AI system must go through rigorous testing before it is deployed to make sure it is secure and dependable. Once it is in use, it must be monitored continuously for performance issues and emerging risks.

Testing acceptance criteria should match identified risks and be clearly documented. All relevant privacy and security safeguards must also apply to AI systems handling sensitive data.

BYOAI is prohibited for sensitive or internal data. Employees and contractors must only use company-approved AI services and models for any data originating from company systems or involving customers, partners, or employees. Exceptions require a documented risk assessment, privacy and security review, contractual safeguards, and formal approval by the Leadership Team and On Q Recruitment's IT provider.

5. Fairness and inclusion

AI system outputs must be inclusive and accessible. They must not involve or result in unfair discrimination against any individual, community, or group. The person responsible for overseeing AI outputs is accountable for ensuring these principles are upheld.

AI use should reinforce our commitments to diversity, inclusion and accessibility – not undermine them. We must be especially careful in use cases where decisions affect individuals from marginalised or vulnerable populations.

6. Transparency and contestability

AI use must be transparent. We must inform impacted parties where appropriate. We must also support them to understand and contest outcomes where relevant.

All approved AI systems must be clearly recorded in On Q Recruitment's AI register. Relevant information about impactful AI-assisted decisions must be retained and, where appropriate, made available upon request.

Impactful AI-assisted decisions are decisions materially influenced by AI outputs where an incorrect, biased, or unreliable result could significantly affect individuals, customers, or On Q Recruitment.

This may include impacts on rights, employment opportunities, access to services, obligations, safety, reputation, or financial outcomes.

These decisions require enhanced controls, including human oversight, testing, documentation, and ongoing monitoring.

7. Human oversight and control

We must maintain human oversight over AI systems. The oversight should be proportionate to how autonomous the AI identified impacts of the AI system are.

Users of AI systems are responsible for overseeing the quality of their outputs. Humans must be able to pause, override or shut down AI systems when necessary. Where critical services rely on AI systems, manual alternatives must be maintained in case the system fails or needs to be taken offline.

Governance and compliance

Roles and responsibilities

To ensure effective governance of AI systems, the following roles and responsibilities are established:

Role	Definition	Responsibilities
AI policy owner	A designated senior leader who is the overall owner for AI, with the authority to govern its use across the organisation. Business Operation Manager	- Champions and maintains the organisation's AI policy and its commitment to responsible AI use. - Holds ultimate accountability for AI governance, including capabilities and risks. - Ensures adequate training is available for those in AI accountability roles
Policy approvers	The individual or committee with the authority to formally approve this policy and its subsequent revisions. This may be a specific person like the CEO or a group like the Board of Directors. Clearly state who holds this authority. CEO and/ or MD	- Reviews and formally approves the AI policy, ensuring it aligns with the organisation's strategic goals, risk appetite, and legal obligations. - Champions the policy from the highest level of the organisation to foster a culture of responsible AI use. - Approves any significant amendments or updates to the policy over time.
Compliance monitor	The individual or team responsible for overseeing and verifying adherence to this AI policy. This function could be assigned to a specific person, an existing team like Internal Audit or Risk and Compliance, or Head of Operations. Business Operation Manager and/ or MD	- Audits AI system documentation to verify that required steps, such as the Pre-Screening Triage and risk assessments have been completed. - Monitors AI-related incident reports and ensures lessons learned are used to improve processes. - Reports on the organisation's overall compliance with this policy to the AI policy owner and governance committee.

Role	Definition	Responsibilities
AI governance committee/ authority	Designated committee or authority responsible for expert consultation and oversight. IT provider	- Provides consultation for AI use cases that are flagged by the screening process. - Acts as the escalation point for reviewing prohibited use cases or other policy disputes. - Reviews and approves high-risk AI systems before deployment.
AI system owner	This is the person accountable for a specific AI system, its entire lifecycle, and its compliance with this policy. Business Operation Manager	Accountable for ensuring their assigned AI systems comply with this policy, including risk assessments, approvals, and documentation.
All employees	All employees, contractors, and other personnel covered by the scope of this policy.	- Adhere to the principles and statements outlined in this policy. - Complete any required AI training to understand the capabilities, limitations and risks of the AI systems they use. - Report any AI-related incidents, hazards or unexpected behaviour through the established channels.

New AI use case procedures

All proposed AI use cases must be screened to identify and flag those that require enhanced governance or pose an unacceptable risk.

This screening process classifies each use case, resulting in an outcome (e.g., *normal*, *elevated*, *prohibited*) that determines the required level of risk assessment, oversight and approval. This ensures our governance effort is always proportionate to the potential impact of the AI system.

Incident management

Any breaches or incidents involving AI must be reported to the **system owner and/ or the compliance monitor** and managed in accordance with our organisation's incident response procedures.

On Q Recruitment will ensure the capacity to take AI systems offline when necessary and will maintain documented manual processes as a fallback to ensure continuity of operations.

Review and Updates

This policy will be reviewed annually, or more frequently if required, to ensure it remains effective and compliant with all applicable laws and regulations.

An ad-hoc review may also be triggered by:

- a significant AI-related incident

- the emergence of new, impactful AI technologies
- changes to relevant laws, regulations, or industry standards.

The review process will be led by the AI policy owner in consultation with the AI governance committee. All substantive changes require formal approval from the policy approvers.

Is there someone I can discuss this policy with?

You can discuss this policy with our On Q Team at onq@onqrecruitment.com.au.